

SECRET  
#4

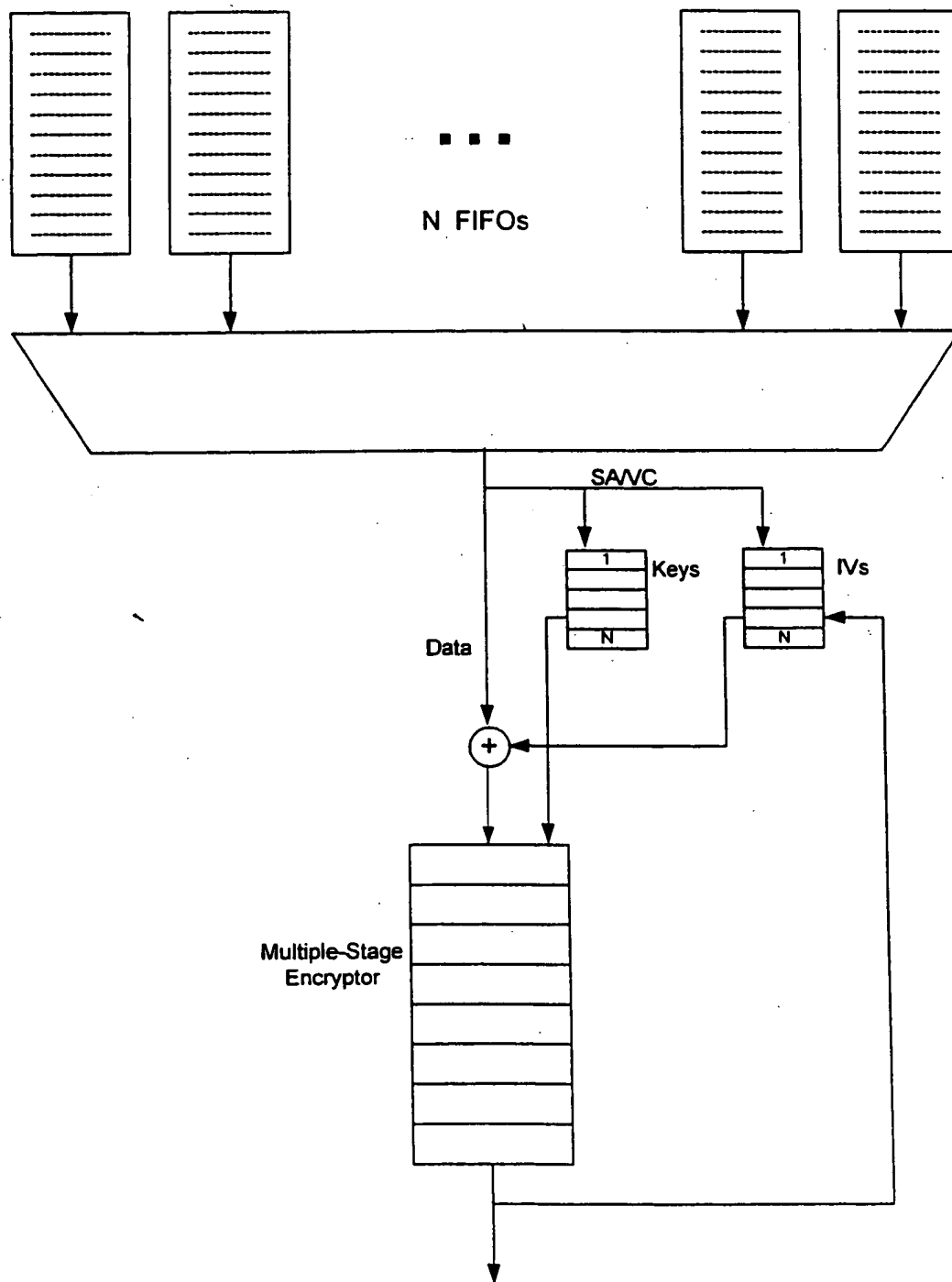
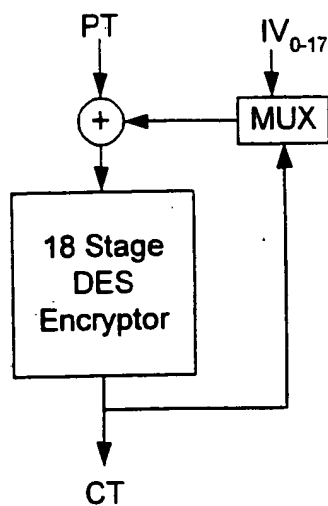


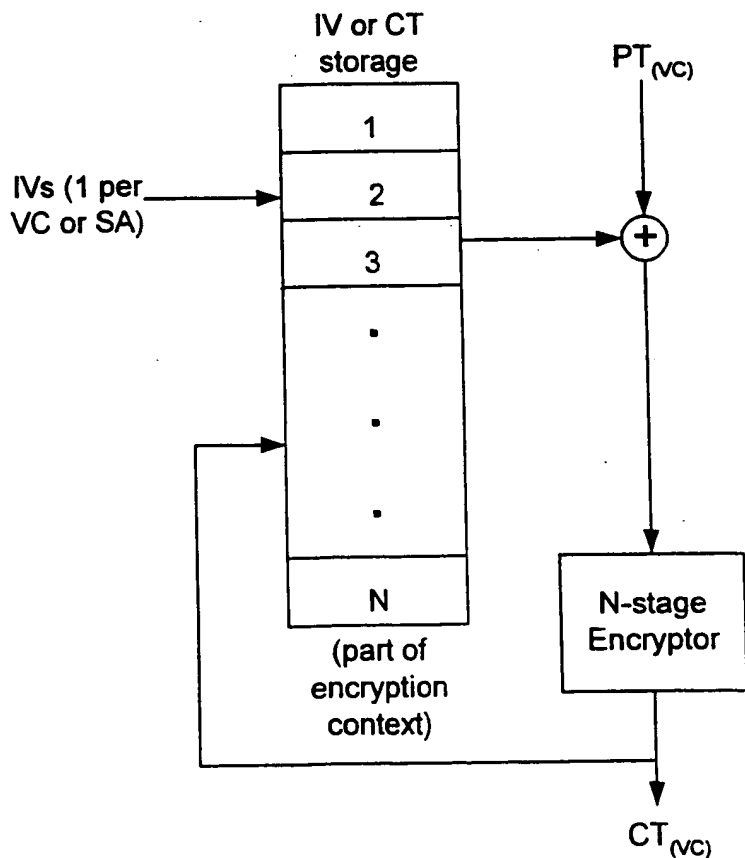
Figure 1

209230-21602650



$$\begin{aligned}
 CT_1 &= E(PT_1 \oplus IV_0) \\
 CT_2 &= E(PT_2 \oplus IV_1) \\
 CT_3 &= E(PT_3 \oplus IV_2) \\
 &\vdots \\
 &\vdots \\
 &\vdots \\
 CT_M &= E(PT_M \oplus IV_{M-1}) \\
 &\vdots \\
 &\vdots \\
 &\vdots \\
 CT_{18} &= E(PT_{18} \oplus IV_{17}) \\
 CT_{19} &= E(PT_{19} \oplus CT_1) \\
 CT_{20} &= E(PT_{20} \oplus CT_2) \\
 &\vdots \\
 &\vdots \\
 &\vdots \\
 CT_N &= E(PT_N \oplus CT_{N-18})
 \end{aligned}$$

Figure 2



$$\begin{aligned}
 CT_{1(VC1)} &= E(PT_{1(VC1)} \oplus IV_{(VC1)}) \\
 CT_{1(VC2)} &= E(PT_{1(VC2)} \oplus IV_{(VC2)}) \\
 &\vdots \\
 &\vdots \\
 &\vdots \\
 CT_{1(VCN)} &= E(PT_{1(VCN)} \oplus IV_{(VCN)}) \\
 CT_{2(VC1)} &= E(PT_{2(VC1)} \oplus CT_{1(VC1)}) \\
 &\vdots \\
 &\vdots \\
 &\vdots \\
 CT_{2(VCN)} &= E(PT_{2(VCN)} \oplus CT_{1(VCN)}) \\
 &\vdots \\
 &\vdots \\
 &\vdots \\
 CT_{M(VCN)} &= E(PT_{M(VCN)} \oplus CT_{M-1(VCN)})
 \end{aligned}$$

Figure 3

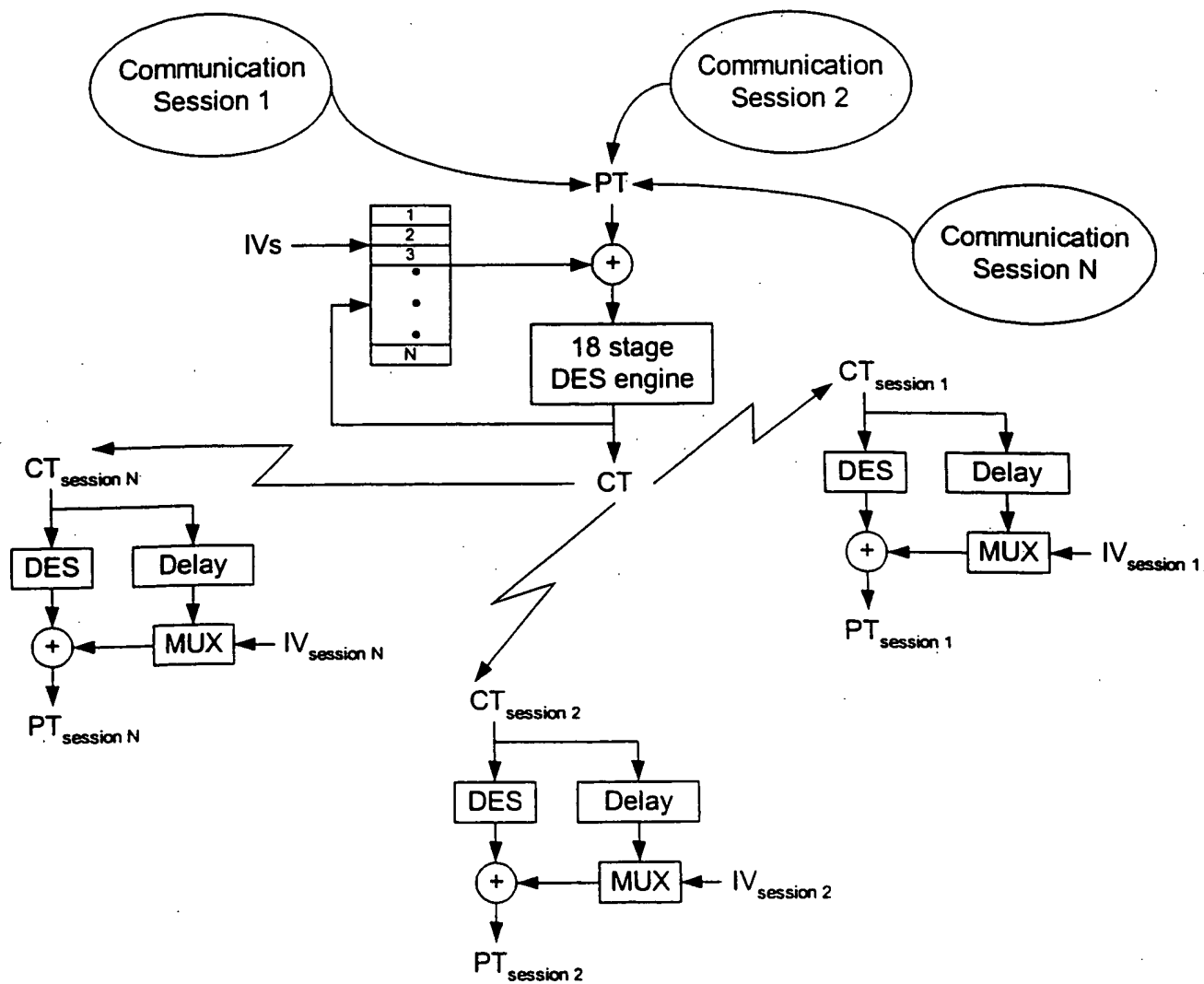


Figure 4

2099230-21607660

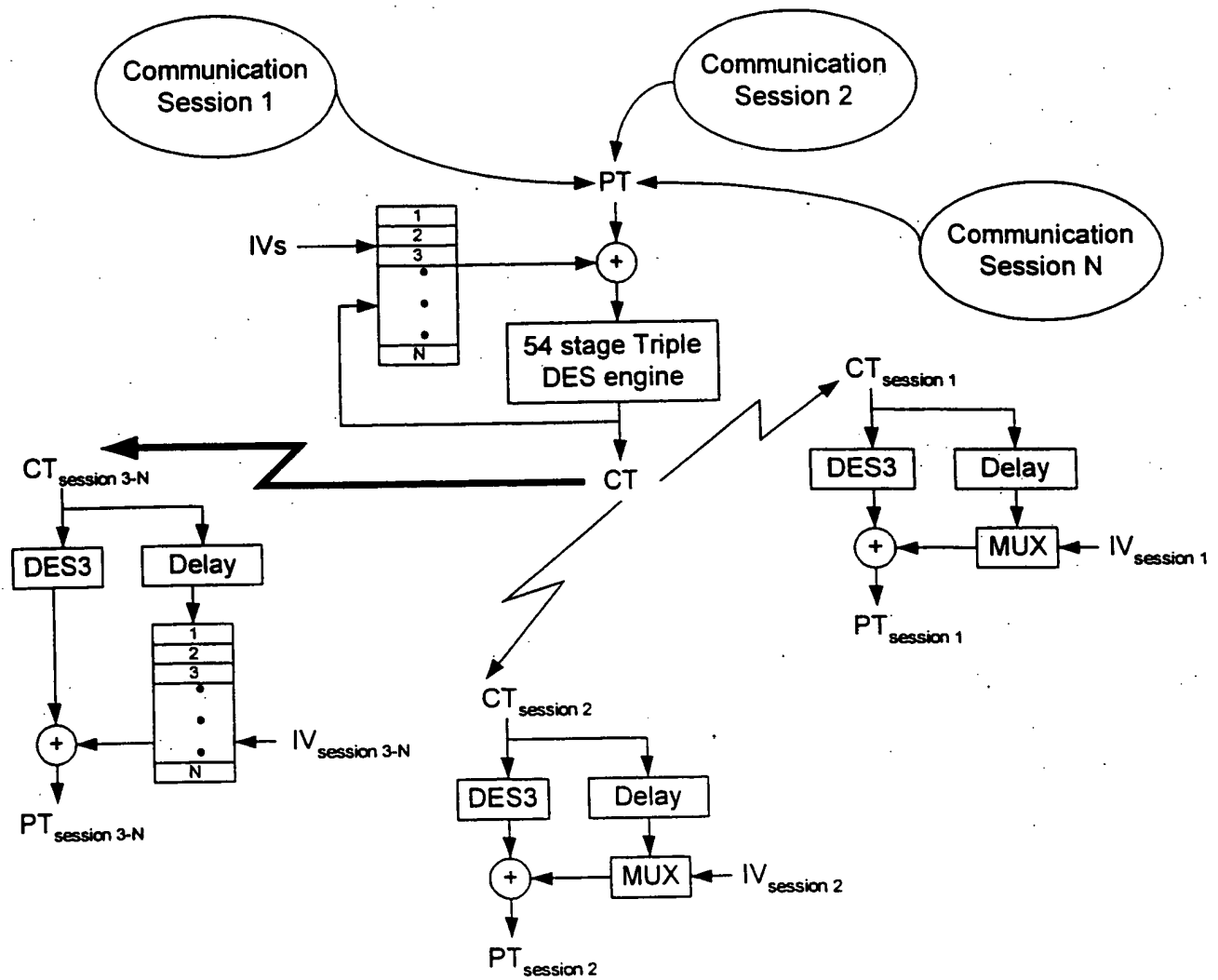


Figure 5

09970912-03660  
209230-21602660

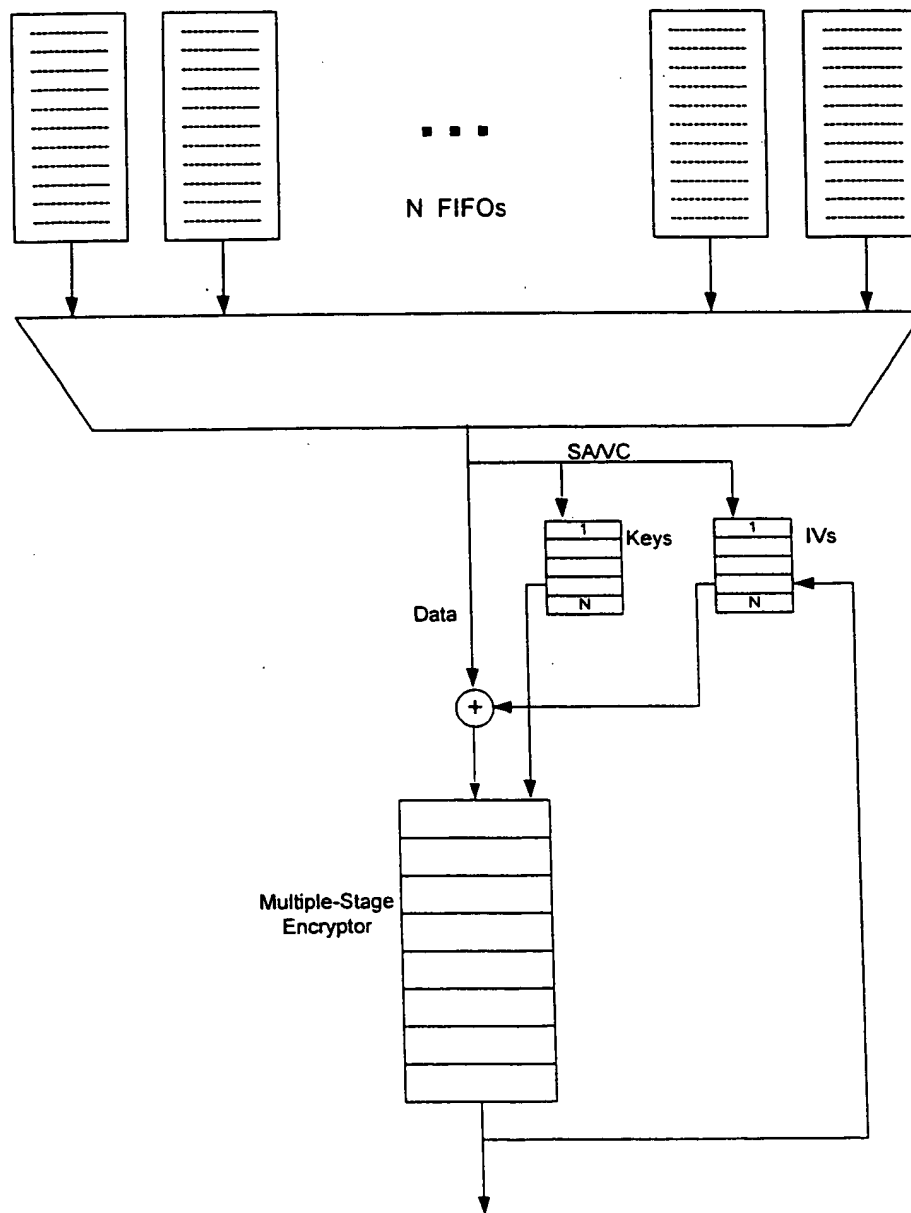


Figure B3.